Volume 49 | Issue 3 Article 5

2004

After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America

R. Bradley McMahon

AFTER BILLIONS SPENT TO COMPLY WITH HIPAA AND GLBA PRIVACY PROVISIONS, WHY IS IDENTITY THEFT THE MOST PREVALENT CRIME IN AMERICA?

I. INTRODUCTION

A. *Nature of the Crime*

Our identities are crucial in conducting our day-to-day transactions. In order to identify us, a majority of institutions use a series of numbers to confirm our identities.[1] Identity theft is the largest and fastest growing crime in the United States.[2] Recently, the instances of identity theft have risen rapidly.[3] Identity theft causes considerable monetary damage because its victims do not realize they are victims for quite some time.[4] In

1. *See* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 665 (1999) (noting importance of one's identity and fact that impersonal numbers, words and other identifiers are all that are needed to prove one's identity).

2. *See* FTC, IDENTITY THEFT SURVEY REPORT 7 (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf [hereinafter FTC REPORT] (finding that 4.6 percent of American adults have been victims of identity theft and extrapolating this data to estimate that 9.91 million Americans have been victims of identity theft in past year); FTC, OVERVIEW OF THE IDENTITY THEFT PROGRAM 8 (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/timelinereport.pdf [hereinafter FTC OVERVIEW] (reporting that complaints filed with FTC Identity Theft Clearinghouse rose from 31,117 annually in 2000 to 131,022 as of July 31, 2003); *see also The Identity Theft and Assumption Deterrence Act: Hearing on S. 512 Before the Subcomm. on Tech., Terrorism and Gov't Info. of the S. Comm. on the Judiciary*, 105th Cong. 3 (1998) (statement of Mari J. Frank) (stating that one in four Americans has been victimized by identity theft); *id.* (opening statement of Chairman Jon Kyl) (stating that Secret Service arrests in 1997 involved crimes that cost financial institutions $745 million in losses); 147 CONG. REC. S12162 (daily ed. Nov. 29, 2001) (statement of Ms. Cantwell) (stating that one in five Americans has either been victim of identity theft or has family member who has been victim); Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1423 (2001) (referring to identity theft as crime of new millennium).

3. *See* Frederick Scholl, *The Changing Privacy and Security Landscape*, 33 BUS. COMM. REV. 54, 54 (2003) ("Previously unheard-of issues relating to digital identity theft, [and] alleged misuse of financial and health-related information . . . have become everyday front-page news.").

4. *See* S. REP. NO. 105-274, at 8 (1998) (noting that MasterCard reported that ninety-six percent of its member banks' fraud losses were attributable to identity theft) (citing GAO report); 147 CONG. REC. S12162 (daily ed. Nov. 29, 2001) (statement of Ms. Cantwell) (stating that it takes twelve months on average before identity theft victim learns of crime); Kenneth M. Dreifach, *Federal and State Enforcement of Consumer Privacy Laws: Focus on Spam, COPPA and Identity Theft*, 748 PRAC. L. INST. 1113, 1119 (2003) (reporting that annual cost estimates of identity theft range up to twenty-seven billion dollars); Hoar, *supra* note 2, at 1425 (noting that Secret Service estimated that identity theft cost financial institutions $745 million in 1997 and that MasterCard reported identity fraud cost its member banks $407 million).

addition, damages from identity theft are difficult to quantify because victims have a ruined credit report, emotional damage and they must often spend hundreds of hours to clear their names.[5] There are thousands of reported and unreported cases of identity theft, many of which have devastated the lives of the victims.[6] Many identity thieves escape prosecution and, consequently, continue to steal the identities of others.[7] Even if law enforcement arrests an identity thief, the victims have little recourse in recovering their lost time and money.[8]

5. *See* Rogan v. City of Los Angeles, 668 F. Supp. 1384, 1387-89 (C.D. Cal. 1987) (relating story of Terry Rogan, whose identity was stolen by killer wanted for double murder, and his plight of being arrested several times at gunpoint because of misconception that he was killer). This exemplifies the emotional damage that may occur when one's identity is stolen and subsequently used to commit crimes. *See* 147 CONG. REC. S12162 (daily ed. Nov. 29, 2001) (statement by Ms. Cantwell) (stating that average victim spends 175 hours to clear name); FTC, Identity Theft Complaint Data, Figures and Trends on Identity Theft January 2000 Through December 2000, *at* http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf (last visited Jan. 4, 2004) (reporting that victims can expect to spend weeks, months or years to restore their names and that many victims suffer devastating effects on their lives); Christopher P. Couch, *Forcing the Choice Between Commerce and Consumers: Application of the FCRA to Identity Theft*, 53 ALA. L. REV. 583, 584-85 (2002) (noting that successful thieves will set up accounts in victim's name using victim's Social Security number and mother's maiden name, leaving victim with debts and eventually ruined credit report).

6. *See* FTC OVERVIEW, *supra* note 2, at 8. (projecting that there will be 210,000 reported cases of identity theft in year 2003); Robert O'Harrow Jr., *Identity Crisis: Meet Michael Berry: Political Activist, Cancer Survivor, Creditor's Dream. Meet Michael Berry: Scam Artist, Killer, and the Real Michael Berry's Worst Nightmare*, WASH. POST, Aug. 10, 2003, at W14 (relating story of Michael Berry, whose identification was stolen by wanted murderer who opened fifteen credit cards in Berry's name; moreover, Berry was arrested because police believed him to be murderer). Berry was finally cleared after thousands of hours of work. *See id.* (stating that Berry spent months correcting his nightmare of identity theft); *see also The Identity Theft and Assumption Deterrence Act: Hearing on S. 512 Before the Subcomm. on Tech., Terrorism and Gov't Info. of the S. Comm. on the Judiciary*, *supra* note 2 (stating that one in four Americans has been victimized by identity theft); Stephen F. Miller, *Someone Out There Is Using Your Name: A Basic Primer on Federal Identity Theft Law*, 50 FED. L. 11, 12 (2003) (relating story of woman who went on vacation only to come home and realize that identity thief had robbed her of $200,000 worth of her personal property by impersonating her, and that statistics indicate that there are thousands of unreported cases of identity theft).

7. *See* S. REP. NO. 105-274, at 7 (reporting that there were 9,500 arrests in 1997 for identity theft). *But see* FTC REPORT, *supra* note 2, at 7 (finding that 4.6 percent of American adults have been victims of identity theft and extrapolating this data to estimate that 9.91 million Americans have been victims of identity theft in past year).

8. *See* S. REP. NO. 105-274, at 11-12 (noting that Act does instruct judges to provide restitution, yet not mentioning time lost and fact that identity thieves may be judgment-proof). Bills have been proposed to address the restitution issue, but not one has been enacted yet. The Senate bill of the Identity Theft and Assumption Deterrence Act provided for restitution, stating that:

> The section makes clear that in determining restitution, any costs and attorney fees should be included. Specifically enumerated costs include those incurred for clearing credit history or rating and those costs in connection with civil or administrative proceedings to satisfy any debt, lien,

This Note will address the effectiveness of congressional acts in deterring identity theft. Part II discusses the nature of identity theft and the congressional acts designed to abate instances of identity theft.[9] Part III addresses the purpose and effectiveness of the Identity Theft and Assumption Deterrence Act of 1998 ("ID Theft Act" or "Act").[10] Part IV addresses the effectiveness of the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) and their attempts to protect personal information.[11] Finally, Part V analyzes the current effectiveness of these laws and suggests reforms based in part on the HIPAA privacy provisions.[12]

II. BACKGROUND

A. *How Identity Theft Occurs*

The easiest and most common way for a thief to steal someone's identity is by acquiring that person's Social Security number and other private information.[13] Social Security numbers are attractive to identity thieves because the numbers are abundant and provide access to a victim's private

---

or other obligations of the victim arising from a defendant's criminal activity.

Id.; *see also* Janice A. Alwin, *Privacy Planning: Putting the Privacy Statutes to Work for You*, 14 DEPAUL BUS. L.J. 353, 363-64 (2002) (noting that federal laws do not provide restitution for consumer victims of identity theft, only for affected financial institutions).

9. For a further discussion of the nature of identity theft and the congressional acts designed to abate instances of identity theft, see *infra* notes 13-28 and accompanying text.

10. The Identity Theft and Assumption Deterrence Act ("ID Theft Act"), 18 U.S.C. § 1028 (2003) (providing for punishment of identity thieves). For a further discussion of the Identity Theft and Assumption Deterrence Act, see *infra* notes 29-53 and accompanying text.

11. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (providing for uniformity in data and privacy in health information); Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 (2003) (providing for identity safeguards in financial industries). For a further discussion of HIPAA and GLBA and their attempts to protect personal information, see *infra* notes 54-186 and accompanying text.

12. For a further discussion of suggested reforms, see *infra* notes 187-255 and accompanying text.

13. *See Protecting Social Security Numbers: Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the Subcomm. on Soc. Sec. of the House Comm. on Ways & Means and the Subcomm. on Immigration, Border Sec. and Claims of the House Comm. on the Judiciary*, 107th Cong. (Sept. 19, 2002), *available at* 2002 WL 31097760 [hereinafter *Hearing*] (statement of Grant D. Ashley, Assistant Director, Criminal Investigative Div., F.B.I.) (stating that possession of Social Security number is key to taking over someone's identity); Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?*, 11 LOY. CONSUMER L. REV. 165, 166 (1999) (noting that Social Security numbers are attractive to thieves because they open up access to bank accounts and other important private information).

information.[14] Social Security numbers commonly are used as a national identifier for everything from car rentals to credit card applications.[15] Often a thief needs only a name and a Social Security number to open up a credit card account or to access an existing account.[16]

A recent study reported that identity theft occurs mainly because information was either stolen or released from a company that compiles personal information.[17] Over one thousand companies compile comprehensive databases of personal information and transfer this information every five seconds.[18] Two of the largest compilers of personal data are the health care and the financial industries.[19] Often, thieves look to these two sources for obtaining personal information.[20] The liberal shar-

14. For a further discussion of how the use of Social Security numbers provides access to a person's personal information, see *Hearing, supra* note 13.

15. *See* 146 CONG. REC. S4334 (daily ed. June 8, 2000) (statement of Sen. Feinstein) (stating that Social Security numbers have become de facto national identifiers used for everything from soldier's number, telephone company accounts and even fishing licenses); Alexander C. Papandreou, Krebs v. Rutgers*: The Potential for Disclosure of Highly Confidential Personal Information Renders Questionable the Use of Social Security Numbers as Student Identification Numbers*, 20 J.C. & U.L. 79, 81 (1993) (noting that Social Security numbers are needed for wide range of activities, such as getting telephone service, using library services, voting, obtaining driver's licenses and banking).

16. *See* Saunders & Zucker, *supra* note 1, at 668 (stating that with name and Social Security number it would be possible to access one's account and change address and then issue cards to new address).

17. *See Use and Misuse of Social Security Numbers: Hearing Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and Means*, 108th Cong. (July 10, 2003), *available at* 2003 WL 21608250 (statement of Chris Jay Hoofnagle, Deputy Counsel, Elec. Privacy Info. Ctr.) (reporting that over fifty percent of identity theft cases occur because personal information is taken from companies that compile personal information); Beth Moskow-Schnoll, *Identity Theft*, 23 U.S. ATTY'S BULL. 25 (Nov. 2001), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab4906.pdf (stating that bank employees often sell personal information for as little as fifteen dollars per account and noting that low-level employees often have access to compilations of personal consumer information).

18. *See* Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1491 (2002) (noting that companies like Metromail Corporation collect over nine hundred pieces of information on individual consumers and that Medical Marketing Service sells over fifty lists of names and addresses of people with various medical conditions to marketers); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000) (stating that companies trade and exchange personal information in United States every five seconds).

19. *See generally* H.R. REP. NO. 106-74, pt. 4, at 120 (1999) (noting that financial services industry is large gatherer of personal information); Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* (1977), *at* http://aspe.hhs.gov/datacncl/1977privacy/c5.htm (last visited Nov. 22, 2003) (stating that insurance industry is one of largest gatherers of personal information).

20. *See* Tyler Chin, *Computer Hackers Access 7,000 Patient Files* (Mar. 24, 2003), *at* http://www.ama-assn.org/amednews/2003/03/24/bisc0324.htm (reporting that 7,000 patient files had been stolen from University of Indiana School of Medicine, which contained sensitive information, including Social Security numbers); *Identity Theft Raises Questions About Security* (Nov. 27, 2002), *at* http://

ing policies of companies allow personal information to flow far beyond primary compilers.[21] Once a person's information is released to one of these central sources, the dissemination of the personal information is completely out of the person's control. The extent to which this information proliferates into third party networks is not known.[22] The information shared by corporate America is one of the principal sources for identity theft.[23]

B. *What Has Congress Done About This Epidemic?*

Congress has recognized the need to protect people's identities and, accordingly, has passed three laws to achieve that end. In 1998, Congress passed the ID Theft Act.[24] The ID Theft Act created strong penalties for identity thieves.[25] In 1996, Congress passed HIPAA.[26] HIPAA went into effect on April 14, 2003, and created strict standards for personal privacy.[27] Lastly, Congress passed the GLBA, which went into effect in 2001, regulating privacy in the financial industry.[28]

III. The Ineffectiveness of the Identity Theft and Assumption Deterrence Act of 1998

A. *Purpose of the ID Theft Act*

Prior to the enactment of the ID Theft Act, the only federal regulations that addressed the issue of identity theft were a patchwork of laws

www.itworld.com/nl/itw_today/11272002/ (reporting theft of sensitive financial information of 30,000 U.S. customers in New York identity theft ring); *see also Red Cross Blood Donors in PA. Are Victims of Identity Theft*, 17 No. 8 White-Collar Crime Rep. 17 (June 2003) (reporting that after patient records were stolen from Philadelphia blood drive, twenty-three patients have been confirmed as identity theft victims).

21. *See* Hatch, *supra* note 18, at 1491 (noting that companies such as MetroMail sell personal information to third parties).

22. *See* Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. Miami L. Rev. 163, 200 (2001) (suggesting that without regulating third party sharing, information could theoretically be recycled and reused forever without consumer's consent).

23. For a further discussion of problems arising from corporate sharing, see *infra* note 56 (discussing case where bank shared credit information that was later used by identity thief).

24. *See* The Identity Theft and Assumption Deterrence Act ("ID Theft Act"), 18 U.S.C. § 1028 (2003) (providing for punishment of identity thieves).

25. *See* 18 U.S.C. § 1028(b)(1)(D) (2000) (punishing those who use another's identification to gain value of more than $1,000, to up to fifteen years in prison).

26. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (providing for uniformity in data and privacy in health information).

27. *See* 66 Fed. Reg. 41316, 41341 (Aug. 7, 2001) (to be codified at 42 C.F.R. pts. 412 & 413) (announcing DHHS's final rule regarding HIPAA and setting compliance date to April 14, 2003).

28. *See* Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 (2003) (providing for identity safeguards in the financial industries).

that aimed primarily to protect or improve accuracy of stored information.[29] These regulations applied to certain industries, and several federal agencies were responsible for their enforcement.[30] The scattered and broad nature of the regulations made prosecution of identity thieves extremely difficult.[31] In response to escalating concerns about identity theft, several states passed laws specifically criminalizing identity theft.[32]

Congress proposed the ID Theft Act in March 1997 in response to the rapid rise of identity theft and the prevalence of dissimilar laws among the states.[33] The purpose of the Act was to criminalize identity theft and to enable law enforcement to target identity thieves before they violated other statutes.[34] The Act carries strong penalties for those convict-

29. *See* Hoar, *supra* note 2, at 1429 (stating that existing laws targeted those who stole identification documents, not those who assumed identities without physical documentation); Saunders & Zucker, *supra* note 1, at 670 (noting that federal consumer protection statutes only offered limited protection for identity theft and that existing laws were only patchwork, primarily designed to ensure informational accuracy and not to combat identity theft).

30. *See* Saunders & Zucker, *supra* note 1, at 670 (noting that several statutes touch upon certain areas, such as disclosure of consumer credit reports without consent and that these statutes were enforced by variety of federal agencies).

31. *See id.* at 669 (noting that while current laws prevent inaccuracy of stored information, they provide little assistance to identity theft victims); *see also* Hoar, *supra* note 2, at 1429 (stating that ID Theft Act was needed because previous laws criminalized use of identification documents but not use of identification information, and that ID Theft Act specifically targets those who fraudulently use personal information regardless of whether information is in printed form); Maureen A. Tighe & Emily Rosemblum, *"What Do You Mean, I Filed Bankruptcy?"—Or How the Law Allows a Perfect Stranger to Purchase an Automatic Stay in Your Name*, 32 LOY. L.A. L. REV. 1009, 1016 (1999) (noting that existing laws viewed victim of crime as creditor and not necessarily person whose identity was stolen and stating that existing laws protect financial institutions more than consumers).

32. *See* S. REP. NO. 105-274, at 6 (1998) (noting that Arizona was first state to make identity theft felony in 1996).

33. *See* Sabol, *supra* note 13, at 168-69 (noting that Congress acted due to growing size of individual and institutional losses arising from identity theft and that crime of identity theft was crossing state lines, exacerbating need for Congress to act as identity theft became more complex); *see also* Ass'n of Am. Physicians & Surgeons v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115, 1126 (S.D. Tex. 2002) (holding that HIPAA falls within congressional Commerce Clause authority to regulate interstate commerce).

34. *See* The Identity Theft and Assumption Deterrence Act ("ID Theft Act"), 18 U.S.C. § 1028(a)(3)(7) (2003) (imposing criminal liability on one who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a felony under any applicable state or local law"). President Clinton also believed the legislation would enable law enforcement to combat identity theft:

> Tens of thousands of Americans have been victims of identity theft. Imposters often run up huge debts, file for bankruptcy, and commit serious crimes. It can take years for the victims of identity theft to restore their credit ratings and their reputations. This legislation will enable the United States Secret Service, the Federal Bureau of Investigation, and

ed.[35] The Act charged the Federal Trade Commission (FTC) with implementing the Act's objectives.[36] The bill as introduced in the Senate provided that those convicted under the statute would be responsible for paying restitution to their victims for their out-of-pocket losses.[37] The House, however, did not pass this provision of the bill.[38] The ID Theft Act became law in 1998.[39]

---

other law enforcement agencies to combat this type of crime, which can financially devastate its victims.

Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007, *reprinted in* 1998 U.S.C.C.A.N. 703, 703 (documenting statement of President William J. Clinton upon signing H.R. 4151).

35. *See* 18 U.S.C. § 1028(b)(1)(D) (2000) (punishing with up to fifteen years in prison those who use another's identification to gain value of more than $1,000); United States v. Wells, 101 F.3d 370, 374 (5th Cir. 1996) (holding that current laws did not adequately account for "extreme personal victimization" of identity theft victims and deciding to depart upward from sentencing guidelines); Hoar, *supra* note 2, at 1431-32 (noting that ID Theft Act has base offense level of "12" because of seriousness of offense, difficulty in quantifying damages and fact that victims often do not realize that their identities have been stolen until certain harms have already occurred); Moskow-Schnoll, *supra* note 17, at 29 (noting that court can make upward departure in offense level if victim suffered serious harm or was erroneously arrested). *But see* Hoar, *supra* note 2, at 1433 (discussing case in which identity thief was sentenced to only twenty-seven months in prison after thief intentionally stole insurance company policyholders' personal information from work and withdrew $764,000 from policyholders' accounts).

36. *See* Centralized Complaint and Consumer Education Service for Victims of Identity Theft, Pub. L. No. 105-318, § 5, 112 Stat. 3007 (2003) (to be codified at 18 U.S.C. § 1028) (stating that within one year of enactment of Act, the FTC is charged with establishing certain procedures). According to the established procedures the FTC is to:

> (1) log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification . . . have been assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act; [and] (2) provide informational materials to individuals described in paragraph (1).

Id.

37. *See* S. REP. NO. 105-274, § 3 (1998) (providing for restitution for victims of out-of-pocket expenses and losses). The bill states that:

> [Restitution] "may include payment for any costs, including attorney fees, incurred by the victim, including any costs incurred—"(1) in clearing the credit history or credit rating of the victim; or "(2) in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as a result of the actions of the defendant."

Id. It is important to note that the proposed Senate bill was not enacted. *See* 18 U.S.C. § 1028 (2003) (lacking text proposed in Senate report).

38. *Compare* S. 512, 105th Cong. (1998) (forcing those convicted under statute to pay restitution to victims for offense relating to identity fraud including payment for any costs by victim, including attorney fees), *with* H.R. 4151, 105th Cong. (1998) (lacking provision for restitution found in Senate bill).

39. *See* 18 U.S.C. § 3663(a)(1)(A) (2003) (permitting court to order restitution for fraud, but not including proposed amendments by Senate to include 18 U.S.C. § 1028).

B. *Why the Act Is Ineffective*

The title "Identity Theft and Assumption Deterrence Act" implies a legislative scheme that will curb the quickly rising tide of identity theft.[40] Identity theft, however, has grown exponentially since the passage of the Act.[41] The Act provides penalties that may suffice to deter, but enforcing its provisions has proven to be difficult.[42] Therefore, the Act's deterrent effect has failed to materialize.[43] The FTC reports that it has distributed 1.2 million copies of its prevention pamphlet to educate the public on identity theft.[44] The FTC's statistics reveal the dramatic rise in identity theft in the United States, a rise that suggests that the public is aware of the crime but is unable to adequately protect itself.[45] Unfortunately for victims of identity theft, even if the thief is apprehended, victims are not compensated for their losses.[46] The Act therefore fails to curtail identity theft because it does not deter thieves, educate consumers or compensate victims.[47]

The ID Theft Act is ineffective because it addresses the wrong side of the problem of identity theft.[48] The Act attempts to deter identity thieves by providing strong penalties.[49] With little chance of being appre-

40. *But see supra* note 2 and accompanying text (discussing rapid rise in identity theft, which occurred after passage of Act).

41. For a discussion of the growth of identity theft, see *supra* note 2 and accompanying text.

42. *See* FTC REPORT, *supra* note 2, at 4 (noting that close to ten million Americans have been victims of identity theft). *But see* Kristen S. Provenza, *Identity Theft: Prevention & Liability*, 3 N.C. BANKING INST. 319, 319 (1999) (reporting that Secret Service has made only 9,500 arrests); Otto G. Obermaier & Ronald R. Rossi, *Evaluating the Crime Legislation by the 105th Congress*, 221 N.Y. L.J. 1, 6 (Jan. 26, 1999) (noting that "the federal law won't deter people because it is too hard to catch these types of criminals").

43. *See* Alwin, *supra* note 8, at 368 (noting that most cases that have been brought under the ID Theft Act have been criminals who have been caught "red handed").

44. *See* FTC OVERVIEW, *supra* at 2 (reporting that over 1.2 million copies of FTC's prevention pamphlet have been distributed since February 2000).

45. *See* FTC REPORT, *supra* note 2, at 12 (noting increasing incidence of identity theft since FTC began compiling statistics on identity theft).

46. *But see* Hoar, *supra* note 2, at 1433 (discussing case where defendant was ordered to pay over $160,000 in restitution to victims after defendant stole Social Security numbers of several high-ranking military officers and applied for credit cards in officers' names). This case is exceptional and not the norm in identity theft prosecutions.

47. *See id.* (discussing case where defendant was ordered to pay over $160,000 in restitution for fraud). For a further discussion of victims' lack of restitution, see *supra* note 35 and accompanying text.

48. *See* Alwin, *supra* note 8, at 367-68 (noting that victim of identity theft is left with no remedy because identity thieves are so hard to catch).

49. *See* 18 U.S.C. § 1028(b)(1)(D) (2000) (punishing those who use another's identification to gain value of more than $1,000 with up to fifteen years in prison).

hended,[50] and the abundance of personal information in the current information age, the risk of suffering a penalty is well worth the reward for a potential thief.[51] Congress should address the problem at the problem's source because the threat of imprisonment will not deter the thief.[52] The source of identity theft is the prevalence of unsecured personal information.[53] To combat identity theft at its source, laws should focus on protecting personal information to stop the flood of identity theft victims.

IV. Congressional Attempts to Protect Personal Information in Two Major Targets for Identity Thieves—The Financial Services and Health Care Industries

A. *The GLBA—Privacy for Financial Institutions*

1. *Overview of the GLBA*

Escalating incidences of identity theft combined with the public's concern for protecting private personal information led Congress to consider drafting legislation on financial privacy.[54] While Congress was nearing a vote on the GLBA regulations, the privacy provisions took on added weight.[55] During this time, Minnesota filed suit against U.S. Bank, alleging that the bank misrepresented to customers that their information was confidential.[56] U.S. Bank sold the customers' information to

50. *See* Obermaier & Rossi, *supra* note 42, at 6 (noting that "the federal law won't deter people because it is too hard to catch these types of criminals").

51. *See* Alwin, *supra* note 8, at 367-68 (noting difficulty in catching identity thief); *see also supra* note 2 and accompanying text (discussing rapid rise in cases of identity theft).

52. *See* Provenza, *supra* note 42, at 326 (suggesting law is weak because it does not focus on methods used by identity thieves to gather information). *But see* Erin M Shoudt, *Identity Theft: Victims Cry Out for Reform*, 52 Am. U. L. Rev. 339, 365 (2002) (noting that credit card companies believe that more aggressive prosecution is solution to identity theft prevention, but noting that they have integral part in prevention).

53. *See* S. Rep. No. 105-274, at 16 (1998) (documenting fears Senator Leahy noted when Congress was considering ID Theft Act; Leahy claimed that protection of personal information is challenge in information age, that criminals commonly get access to personal information of others and use such information to commit crimes and that thieves can gather information from large centralized sources of personal information).

54. *See* Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 Tex. Int'l L.J. 421, 442 (2002) (arguing that cases where banks revealed private information to third parties prompted outcry from privacy advocates and caused Congress to enact GLBA privacy provisions).

55. *See* Charles M. Horn, *Financial Services Privacy at the Start of the 21st Century: A Conceptual Perspective*, 5 N.C. Banking Inst. 89, 93-100 (2001) (discussing increased pressure on Congress to enact privacy legislation).

56. *See* Eric Poggemiller, *The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. Banking Inst. 617, 618 (2002) (discussing case initiated by Minnesota against U.S. Bank, in which U.S. Bank allegedly sold information to telemarketers in violation of consumer protection laws, and noting case was settled shortly after it was filed).

telemarketers, who used the information to make fraudulent charges.[57] The public soon realized that most large banks also routinely sold personal information, leading to increased pressure on Congress to adopt privacy protections.[58] In enacting the GLBA, Congress set forth the most stringent privacy regulations ever enacted for the financial industry.[59] The GLBA reflects "the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[60] At least one court has upheld the GLBA on constitutional grounds as a legitimate method for furthering Congress's intent.[61] The GLBA gave financial institutions until July 1, 2001, to comply with its regulations, which included mandatory notice requirements of policy,[62] as well as opt-out requirements to the sharing of nonpublic information with third parties.[63]

The GLBA is sweeping because it applies to "financial institutions." Interestingly, Congress did not clearly define this term in the Act.[64] The FTC has defined the scope of the Act, and in a recent case, a court held that the FTC's definition is entitled to deference.[65] Financial institutions

57. *See id.* at 618 (explaining that telemarketers that bought information from U.S. Bank used information to commit fraud by debiting customer accounts without customers' authorization); *see also* Loring, *supra* note 54, at 442 (stating that third party telemarketers debited consumers' accounts without consumer knowledge or authorization).

58. *See* Poggemiller, *supra* note 56, at 618 (noting that lawsuit drew national attention to privacy issue when it became apparent that most large banks routinely sold personal information, causing Congress to amend GLBA to include banking privacy provisions).

59. *See* Loring, *supra* note 54, at 443 (stating that GLBA regulations contain most extensive privacy regulations in history and that regulations are affirmative and ongoing obligation).

60. 15 U.S.C. § 6801(a) (2003).

61. *See* Individual Reference Servs. Group v. FTC, 145 F. Supp. 2d 6, 43 (D.D.C. 2001) (holding that GLBA regulations prohibiting disclosures without consent clearly advance congressional intent).

62. *See* 16 C.F.R. § 313.4(a) (2003) (requiring financial institutions to provide clear and conspicuous notice to customers initially as well as annually); R. Shane McLaughlin, *The Gramm-Leach-Bliley Financial Modernization Act—Analysis & Suggestions for Reform*, 72 Miss. L.J. 1099, 1102 (2003) (stating that GLBA requires financial institutions to supply customers with privacy policy at outset of relationship and that annual privacy notices must be sent to consumers, but that annual privacy notices are not required to be sent to former customers).

63. *See* 16 C.F.R. § 313.6(a)(b) (2003) (requiring privacy notice to contain customer's opt-out rights); McLaughlin, *supra* note 62, at 1104 (explaining that privacy notice must state consumer's right to opt out of disclosures as well as instructions on how to exercise that right).

64. *See* 16 C.F.R. § 313.3(k)(1) (2003) (defining financial institution as business that is "significantly engaged" in financial activity).

65. *See* Trans Union v. FTC, 295 F.3d 42, 49-51 (D.C. Cir. 2002) (holding that Trans Union, as credit reporting agency, was subject to provisions of GLBA and that FTC is authorized to define personally identifiable financial information). The court also decided to defer to the FTC's definition. *See id.* at 49.

under the Act include everything from real estate appraisers to automobile dealerships.[66] Entities covered under the Act must meet specific requirements before they may disclose an individual's personal information to a nonaffiliated third party.[67] Congress intensely debated the types of requirements for various third parties prior to the passage of the Act.[68]

One fundamental disagreement in Congress revolved around whether the Act should establish an opt-out or an opt-in system. In an opt-out system, information can be shared unless the consumer opts out of the sharing.[69] Under an opt-in system, no sharing can take place until the

---

66. *See* 16 C.F.R. § 313.3(k)(2) (2003) (giving examples of financial institutions such as retailer that extends credit, real estate appraiser, automobile dealership that leases cars, career counselors that place individuals into financial organizations, business that prints checks for consumers, business that wires money, check cashing business, accountant, travel agency operating in connection to financial services, mortgage broker and investment advisor); *id.* § 313.1(b) (classifying "mortgage lenders, 'pay day' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors" as financial institutions).

67. *See id.* § 313.10 (mandating that before entities may disclose personal information, entities must send initial notice, annual notice and opt-out notice, and customer, after reasonable period of time, must fail to opt out); *see also* Horn, *supra* note 55, at 101 (noting that above privacy regulations do not apply to affiliates of covered entities, third parties that perform certain services for covered entity and third parties that engage in marketing of products related to covered entity).

68. *See* 145 CONG. REC. S13894 (daily ed. Nov. 4, 1999) (statement of Sen. Shelby). According to Senator Shelby:

> The so-called privacy protection of customers being given an opportunity to "opt-out" clearly demonstrates the corporate benefits this bill intends. If this bill will benefit consumers, let the corporations sell themselves by mandating that consumers must "opt-in" to have information on themselves shared or sold. Financial literacy is already faced with a plethora of challenges let alone teaching consumers how to search for obscure fine print to protect privacy.

Id. Senator Shelby also noted:

> I believe these privacy provisions are a sham. I have said it before. They are a joke on the American people, and I will not sit by and be a party to this. When the American people, and they will, become aware of what Congress has done, it will be too late.

Id.; *see also* 145 CONG. REC. S13786 (daily ed. Nov. 3, 1999) (statement of Sen. Gramm) (referring to notice requirement). Senator Gramm noted that:

> This is important because this is the ultimate protection of privacy. If I do not believe a bank protects my privacy, I do not want to bank with them. I can bank with somebody else. If millions of people feel the way I do, you will get banks that will set out policies of not sharing information, and they will attract customers.

Id.

69. *See generally* J. Stephen Zielezienski, *Insurance Privacy After Gramm-Leach-Bliley—Old Concerns, New Protections, Future Challenges*, 8 CONN. INS. L.J. 315, 320 (2002) (defining "opt out" so that information is shared unless consumer affirmatively indicates otherwise).

consumer opts in.[70] Opt-in supporters did not want consumers to have to struggle through long documents of fine print to protect their privacy.[71] The supporters of the opt-out standard argued that consumers had plenty of freedom to choose not to have their personal information shared.[72] The financial industry supported the opt-out standard because it claimed that information sharing was a necessary business practice and that the costs associated with an opt-in system would be passed on to consumers.[73] Information sharing allows financial institutions to make strategic decisions, offer low risk, preapproved credit cards and create a database of personal information, which may be sold for income.[74]

The second controversy during the passing of the GLBA concerned whether a financial institution could disseminate personal information to

---

70. *See id.* at 326 (defining "opt in" so that information is not shared unless consumer expressly grants consent to share information).

71. *See* 145 CONG. REC. H11539 (daily ed. Nov. 4, 1999) (statement of Rep. Davis) (noting benefits that opt-in system brings to consumers by allowing them to keep privacy without having to read through obscure fine print); Poggemiller, *supra* note 56, at 630 (noting that some of opt-out notices were ten pages long because companies wanted low response rate).

72. *See* 145 CONG. REC. S13785 (daily ed. Nov. 3, 1999) (statement of Sen. Gramm) (noting beneficial services that are possible from opt-out system, stating that he does not get Neiman Marcus catalogs because Neiman Marcus already knows that he does not purchase luxury items and that society benefits because Neiman Marcus does not print expensive and unnecessary catalogs for those who would not purchase anything); *id.* at S13786 (noting that opt-out provision allows consumer to evaluate privacy policies of institutions, and if consumers are not satisfied, they can take business elsewhere, and if millions of people feel same way, banks will revise privacy policies in ways to attract customers).

73. *See* Ayca Ergeneman, *The Devastating Effect of Opt-In Restrictions*, ¶ 2, *at* http://www.aba.com/Industry+Issues/GR_PR_Opt-in.htm (last visited Nov. 25, 2003) (stating that "opt-in to information sharing decreases the speed, lowers the efficiency, and raises the cost of information"); *id.* ¶ 3 (providing example of when mortgage company would have to start from scratch to collect and verify information of loan applicant). *But see* Beth Givens, *Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act*, ¶¶ 53-55, *at* http://www.privacyrights.org/ar/fin_privacy.htm (last visited Nov. 25, 2003) (arguing that costs of opt-in and opt-out notices are similar and that costs of requirements need to be balanced against personal and societal costs of fraud that occur when information is misused).

74. *See* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 506 (2002) (providing multiple reasons why financial institutions want freedom to collect personal information, and suggesting that information is valuable in its own right); Chris Jay Hoofnagle, *GLB: More Protections Needed to Ensure Financial Privacy*, SH060 ALI-ABA 199, 201 (2003) (stating that fair information principles set forth by Organization of Economic Cooperation and Development imply that data collectors should only collect minimum amount of data necessary for transaction, and noting that principles also prohibit sharing information gathered for one purpose for another purpose without consent). Nevertheless, there may be benefits for financial institutions that minimize their data collection, such as simpler privacy policies. *See id.* at 201 (noting that in addition to the benefits of simpler privacy policies, institutions may also benefit from collecting less information that could be misused).

its affiliates.[75] Supporters argued that allowing financial institutions to share information with affiliates provided the consumer with the valuable resource of one-stop shopping.[76] Those who opposed affiliate sharing were shocked that a large financial company could share nonpublic personal information with "affiliated telemarketers selling non financial products such as travel services, dental plans, and so forth."[77]

The House version of the GLBA provided for extensive privacy provisions.[78] While congressional disagreement threatened the successful passage of the GLBA, President Clinton signed it into law with limited privacy provisions.[79] Eventually, the GLBA passed with an opt-out requirement, with several notable exceptions.[80] The GLBA does not require opt-out notices when information is shared to perform services for the financial institution.[81] Financial institutions may also share nonpublic information

---

75. *See* Therese G. Franzen & Leslie Howell, *Financial Privacy Rules: A Step by Step Guide to the New Disclosure Requirements Under the Gramm-Leach-Bliley Act and the Implementing Regulations*, 55 CONSUMER FIN. L.Q. REP. 17, 19 (2001) (defining affiliate as company that controls, is controlled by or is under same control as another company).

76. *See* Jack Cooksey, *Private Matters: Does the Law Go Far Enough to Protect Privacy?*, *at* http://www.insidebiz.com/hamptonroads/special_report/special082800 (last visited Nov. 25, 2003) ("[W]hen you do business with First Union, you expect to be able to do business with all of First Union.").

77. 145 CONG. REC. S13894 (daily ed. Nov. 4, 1999) (quoting statement of Sen. Shelby) (stating that "large financial conglomerates will have more information on citizens than the IRS, but [Congress has] done virtually nothing to protect the sharing of such nonpublic personal financial information for the American people").

78. *See* H.R. 10, 105th Cong. (1999) (including restrictions of access to consumer information by affiliates); 145 CONG. REC. S13783, 13789 (daily ed. Nov. 3, 1999) (statement of Sen. Sarbanes) (pointing to lack of privacy protections in Senate bill).

79. *See* Kristina A.K. Hickerson, *Consumer Privacy Protection: A Call for Reform in an Era of Financial Services Modernization*, 53 ADMIN. L. REV. 781, 784 (2001) (noting that House version had much stricter privacy provisions but disagreement in Congress threatened Act, with Clinton administration signing much weaker version into law while asserting that administration would take steps to create more comprehensive consumer protection); *id.* at 792 (noting that House reluctantly approved Senate version of bill because of importance of overall Act); *see also* 145 CONG. REC. E2306 (daily ed. Nov. 8, 1999) (statement of Rep. Costello) (stating fear that bill's limited privacy protections would cause "the walls protecting our financial privacy and other personal information [to] slowly [be] eroded").

80. *See* Hickerson, *supra* note 79, at 783-84 (discussing GLBA provisions).

81. *See* 15 U.S.C. § 6802(b)(2) (2003) (requiring financial institution to contract with third party to keep information confidential and to notify customers that it engages in such practices). The statute states:

> This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions . . . .

Id. (describing exception).

with their affiliated third parties without sending an opt-out notice to the consumer.[82] Although the GLBA covers a broad range of entities and provides harsh penalties for noncompliance,[83] its protection of private personal information is minimal.[84] The flaws in the Act occurred because congressional debate weakened a vast amount of the privacy provisions.[85]

2. *Why Has the GLBA Proven Ineffective in Protecting Personal Information from Theft?*

This great initiative to protect personal information was drafted with many loopholes, which in practice give consumers little control over their private personal information. There are five main weaknesses in the Act: (1) the GLBA does not properly define what personal information is covered under the Act; (2) receiving notices of privacy policies does little to enhance privacy; (3) consumers have no control over information disseminated to affiliates; (4) consumers have only limited control of the dissemination of information to third parties via an opt-out notice; and (5) although the GLBA carries tough penalties, victimized consumers have no cause of action.[86]

a. The GLBA Only Covers Nonpublic Information

The GLBA only applies to "nonpublic information," meaning information that is not readily available to the public.[87] Information is considered public if a financial institution has a reasonable basis to believe that the information is lawfully available to the public.[88] Therefore, informa-

82. *See id.* § 6802(a) (requiring opt-out notice only when sharing information with nonaffiliated third party); Horn, *supra* note 55, at 100-01 (noting that privacy provisions do not apply to affiliates or to third parties who perform services for covered entity).

83. *See* 15 U.S.C. § 6823(b) (2003) (stating that violations "involving more than $100,000 in a 12-month period shall be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of Title 18, imprisoned for not more than 10 years, or both"); *see also* 18 U.S.C. § 3571(b)-(c) (2003) (calling for penalties of up to $250,000 for individuals and $500,000 for organizations).

84. *See* Cuaresma, *supra* note 74, at 511 (discussing weaknesses of GLBA).

85. *See generally* Hickerson, *supra* note 79, at 791-92 (highlighting congressional debates over GLBA).

86. *See generally* Cuaresma, *supra* note 74, at 510 (outlining most accepted flaws with GLBA).

87. *See* 16 C.F.R. § 313.1 (2003) (stating that GLBA only applies to sharing of nonpublic information); *id.* § 313.3(n) (stating that nonpublic personal information means: "(i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available").

88. *See* Cuaresma, *supra* note 74, at 511 (stating that information is public if it can be obtained by government records or widely distributed media); *see also* 16 C.F.R. § 313.3(n) (2003) (giving example of public information as "list of individuals' names and addresses that contains only publicly available information, is not

tion that the public can obtain through widespread media, such as the Internet, is not protected under the GLBA.[89] For example, a nonfinancial institution could share with a financial institution a list of names, addresses, phone numbers and other readily available information, and then compile it with existing personal information to create a more detailed profile.[90] The effect of covering nonpublic information instead of personal information is that financial institutions can share larger and more detailed consumer profiles.[91] Critics of the GLBA argue that the Act should protect public information if the consumer desires to protect this information.[92] As information becomes ubiquitous online, a personal profile can be built in minutes at little cost, raising privacy concerns that did not exist in the world of paper financial records.[93] The further that personal information proliferates into third party networks, the greater the risk of identity theft.[94]

b. Notices Do Not Enhance Privacy

Receiving initial and annual privacy notices may provide consumers with insight into the personal-information-sharing practices of companies,

---

derived, in whole or in part, using personally identifiable financial information that is not publicly available").

89. *See* Cuaresma, *supra* note 74, at 511 (noting that FTC acknowledged that information on Internet site is considered public if site is available to general public).

90. *See* Pandozzi, *supra* note 22, at 197 (noting that public information could then be compiled using information that financial institutions have and such information could be shared with third parties). *But see* Trans Union v. FTC, 295 F.3d 42, 51 (D.C. Cir. 2002) (holding that nonpublic information includes all information disclosed to financial institution for purpose of transaction, including names, addresses and Social Security numbers).

91. *See* Pandozzi, *supra* note 22, at 197 (explaining how financial institutions share information with third parties).

92. *See Financial Privacy: Hearing on Emerging Financial Privacy Issues Before the House Comm. on Banking and Fin. Inst. and Consumer Credit*, 106th Cong. ¶ 16 (1999), *available at* http://financialservices.house.gov/banking/72099cul.htm (last visited Nov. 25, 2003) (prepared statement of Dr. Mary Culnan) (noting that people try to prevent disclosure of public information). Dr. Culnan noted:

> The telephone book, one of the most widely available sources of public information, is a good example that people value the ability to make choices about disclosing even their name and address, and when offered choices . . . [c]onsumers should be able to opt out of having their names and addresses shared for marketing purposes . . . .

93. *Id.*

See Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 638 (2002) (stating that proliferation of online information allows profile of individual to be built at minimal cost, raising concerns about risk to privacy that did not exist when society was based on paper record-keeping system).

94. *See* Hoofnagle, *supra* note 74, at 206 (noting that every time information is shared, opportunity for identity theft increases).

but large loopholes render the notices completely ineffective.[95] The purpose of the notice requirement was to allow consumers to take control over what a bank did with their information, and if they did not like the bank's policy, they could take their business elsewhere.[96] The largest loophole in the notice requirement is that it does not apply to former customers.[97] Therefore, if customers are dissatisfied and take their business elsewhere, the institution could share all the personal information that it had previously compiled.[98] In effect, consumers retain no control over what happens to their personal information.

Further, the notices themselves do not adequately inform consumers about what is shared and who the recipients are.[99] According to the chairman of the FTC, "[a]cres of trees died to produce a blizzard of barely comprehensible privacy notices."[100] Institutions have sent out approximately 2.5 billion privacy notices as of June 2001, costing between two and five billion dollars in printing costs alone.[101] The average home receives between twenty and fifty annual notices, lessening the chances that people read the notices.[102]

c. Financial Institutions Can Share Anything with Affiliates

Under the GLBA, financial institutions are free to disclose any consumer personal information to their affiliates, giving consumers no con-

95. *See generally* Franzen & Howell, *supra* note 75, at 20 (outlining general privacy notice guidelines).

96. *See* 145 CONG. REC. S13883 (daily ed. Nov. 4, 1999) (statement of Sen. Edwards) (stating that this is most powerful tool that consumers have over their privacy); *see also* Franzen & Howell, *supra* note 75, at 20 (noting that initial notices are not even required for consumers who do not have continuing relationship with institution).

97. *See* 15 U.S.C. § 6803(a) (2003) (stating that disclosures are made when consumer relationship is established); Horn, *supra* note 55, at 110 (noting that GLBA annual notice requirement does not apply to former customers).

98. *See* 15 U.S.C. § 6803(a) (2003) (providing that regulations only apply when consumer relationship is established); Cuaresma, *supra* note 74, at 512 (noting that by taking business elsewhere, there is not limitation on sharing of information that has already been gathered); Horn, *supra* note 55, at 105 (defining consumers versus customers).

99. *See* Hoofnagle, *supra* note 74, at 203 (stating that notices do not contain enough specificity to adequately inform consumers and that companies often tried to hide privacy issue by reassuring customers that information would only be shared with trusted and family companies); *see also supra* note 71 and accompanying text (noting difficulty in reading privacy notices).

100. Robert W. Hahn, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 130 (2002) (quoting chairman's statement concerning Act).

101. *See id.* at 130-31 (noting that forty thousand financial institutions mailed 2.5 billion notices to consumers by June 2001); *id.* at 145 (noting that printing costs alone from GLBA are between two and five billion dollars).

102. *See id.* at 130-31 (noting that consumers received 2.5 billion notices by June 2001, with each home receiving twenty to fifty). Fleet's chief privacy officer believes that these notices are going unread because consumers are being inundated with such notices. *See id.* at 131.

trol over their information.[103] The GLBA does not require institutions to notify consumers about this type of sharing.[104] For example, once a bank obtains personal information, it may share this information with its insurance, brokerage or credit affiliates.[105] With the advent of large mergers of multifaceted corporations, there is essentially no limit on who may be an affiliate.[106] Therefore, information can be disseminated far beyond what consumers imagine.[107] For example, Charter Pacific Bank was caught selling 3.6 million credit card files to a convicted felon.[108] Charter Pacific had compiled the numbers from transactions that occurred at other affiliate banks, without notice to consumers.[109]

d. An Opt-Out Provision for Third Parties Is Ineffective

Very few consumers choose to opt out of sharing their personal information with third parties.[110] The low response rate is largely due to the difficulty of the process of opting out.[111] Because financial institutions have no incentive to facilitate the process of protecting information, the opt-out process is usually quite cumbersome.[112] A typical opt-out notice is

103. *See* Cuaresma, *supra* note 74, at 512 (explaining that "customers cannot opt-out of information sharing between affiliates").

104. *See id.* (noting that affiliate sharing is not subject to GLBA privacy notice requirements).

105. *See id.* (noting range of possible companies where one's information could be shared). For example, one entity may have affiliates in the insurance, banking and securities industries, and there is no roadblock for exchanging information once it is acquired. *See id.*

106. *See id.* (noting wide range of affiliate possibilities).

107. *See* Pandozzi, *supra* note 22, at 199 (noting that consumers may misinterpret GLBA privacy provisions, not realizing that they do not apply to numerous affiliates of financial institution).

108. *See Fair Credit Reporting Act and Affiliate Sharing Practices: Testimony Before the S. Banking, Hous., and Urban Affairs Comm.*, 108th Cong. (June 26, 2003), *available at* 2003 WL 21481585 (statement of Edmund Mierzwinski, Consumer Program Dir., U.S. Pub. Int. Group) (noting that Charter Pacific had sold database of credit card numbers to convicted felon who later made fraudulent charges to those credit cards).

109. *See id.* (stating that Charter Pacific did not create database of credit card numbers from its own customers but compiled it with information from affiliate merchants of Charter Pacific).

110. *See* Poggemiller, *supra* note 56, at 627-30 (noting low opt-out response rate, and discussing why consumers failed to opt out).

111. *See infra* note 112 and accompanying text (discussing how companies make it difficult for consumers to opt out).

112. *See* Cuaresma, *supra* note 74, at 513 (illustrating process that companies make consumers go through to opt out). For example, companies might make customers request a form, wait for it to arrive via mail and then send it back via mail. *See id.* (describing opt-out process); *see also* Hoofnagle, *supra* note 74, at 204 (reporting that evidence suggests that institutions are actively frustrating the opt-out process). For example, many credit card companies make the consumer send an opt-out form to a different address than where the payment is sent. *See id.* (noting how companies frustrate opt-out process). A current petition calls for easier opt-out procedures such as availability of toll-free numbers, web sites and check

long, written in fine print and dense legalese.[113] Although the opt-out notices are supposed to be clear,[114] most are written on a college or graduate level and contain complicated sentences and uncommon words.[115] The opt-out notices attempt to persuade the consumer into thinking that sharing information will bring benefits.[116] For example, the notices include phrases such as "[i]n order to provide you with better products and services."[117] In *Ting v. AT&T*,[118] a California federal court found that AT&T conducted research to determine how to draft notices that the consumer would likely ignore.[119]

Further, a financial institution can disclose information to a third party if it performs services for the financial institution.[120] The financial institution's only obligation is to contract with the third party to keep the

---

boxes on postcards to facilitate the process. *See id.* at 203 (describing petition to reform opt-out procedures).

113. *See* Poggemiller, *supra* note 56, at 630 (noting that some opt-out notices were ten pages long because companies wanted low response rate); *see also* 145 CONG. REC. H11539 (daily ed. Nov. 4, 1999) (statement of Rep. Davis) (stating that consumers had to sift through privacy notices that were difficult to read).

114. *See* 16 C.F.R. § 313.5(a)(1) (2003) (stating that annual privacy notices under GLBA must be clear and conspicuous notice of privacy policies).

115. *See* Poggemiller, *supra* note 56, at 629 (noting use of complicated language in opt-out notices written by financial institutions, resulting in some receiving a grade of D or F in report by USAction); Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices* (July 2001), *at* www.privacyrights.org/ar/GLB-Reading.htm (reporting that study of sixty privacy notices revealed that they were written on third or fourth year college level and twelve were written on graduate level; all were rated "difficult" and eighteen were rated "very difficult"). It is recommended that privacy notices be written at a junior high school level. *See id.* (explaining that literacy experts recommend that this is appropriate reading level for consumers).

116. For a discussion of the persuasive nature of privacy notices that attempt to get consumers to share their personal information, see *infra* note 117 and accompanying text.

117. Tena Friery & Beth Givens, *Financial Privacy Notices: Do They Really Want You to Know What They're Saying?* (June 2001), *at* http://www.privacyrights.org/ar/GLB-CodeOpEd.htm (arguing that companies use such language in opt-out notices as marketing ploy to get customers to consent to sharing information); *see also* Hoofnagle, *supra* note 74, at 204 (noting that financial institutions try to persuade customers not to opt out by stating that information will only be shared with "trusted" or "family" corporations).

118. 182 F. Supp. 2d 902 (N.D. Cal. 2002).

119. *See id.* at 913 (finding that AT&T discovered that by indicating in boldface type that what is contained in notice does not affect billing, most customers would stop reading). The AT&T notice in boldface at the top of the document read, "Please be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to do." *Id.*

120. *See* 16 C.F.R. § 313.11(a)(iii) (2003) (allowing third parties who perform service to disclose information in ordinary course of business of providing service); Pandozzi, *supra* note 22, at 200 (noting that disclosures may be made to third parties who provide services as long as notice of this type of disclosure is included in financial institution's initial privacy notice). *But see* Horn, *supra* note 55, at 113 (suggesting that notice requirement may be met by stating that information will be shared to extent allowed by law).

information private.[121] Therefore, an institution could share with anyone as long as it and the third party had a contractual agreement, thereby bypassing the entire opt-out provision.[122] Third parties could then transfer the information and a consumer's private information would circulate *ad infinitum*, effectively removing all control of personal information from the consumer.[123] In addition, a recent district court decision held that a customer must opt in before institutions can share their information for a subpoena.[124] Arguably, this precedent enables a financial institution to share a consumer's information with an affiliate or contracted third party easier than it can share the information with a court of law.

e. No Private Cause of Action for Violations

The GLBA does not give citizens a private cause of action if institutions share their information in a manner that violates the GLBA.[125] Only the FTC has the right to enforce the GLBA privacy provisions.[126] Currently, the GLBA regulates abusive privacy practices instead of addressing individual financial institution infractions.[127] For example, in *Menton v. Experian Corp.*,[128] the court held that the victim had no cause of action

121. *See* 16 C.F.R. § 313.13(a)(1)(ii) (2003) (requiring contractual agreement to keep information private and prohibiting disclosure of information for purposes other than to carry out purposes for which information was disclosed); Pandozzi, *supra* note 22, at 200 (noting that contractual agreement requires third party to maintain confidentiality of information provided to it by covered entity).

122. *See* Pandozzi, *supra* note 22, at 200 (noting that "a financial institution may entirely circumvent [the GLBA] by entering into contracts with third party service providers"); *see also* Horn, *supra* note 55, at 113 (suggesting that financial institutions may be able to contract with third parties without adequately informing consumer by simply stating that consumer information will be shared to extent allowed by law).

123. *See* Pandozzi, *supra* note 22, at 200 (arguing that, unknown to consumer, third party services and marketing exceptions could theoretically allow third parties to reuse information and retransfer personal information to more nonaffiliated third parties, thus bypassing all GLBA privacy protections).

124. *See* Union Planters Bank v. Gavel, No. CIV.A.02-1224, 2002 WL 975675, at *6 (E.D. La. May 9, 2002) (holding that, based on GLBA, bank was preliminarily enjoined from releasing customer's information without consent).

125. *See* Cuaresma, *supra* note 74, at 514 (noting that GLBA does not provide victims with private cause of action).

126. *See* 16 C.F.R. § 313.1(b) (2003) (stating that FTC has enforcement authority over financial institutions); Cuaresma, *supra* note 74, at 514 (noting that enforcement consists of correcting abusive practices instead of reconciling individual rights harmed by infractions and that federal and state agencies, including FTC, are responsible for addressing infractions by institutions).

127. *See* Cuaresma, *supra* note 74, at 514 (noting that under current enforcement, financial institutions have little incentive to comply because consumers whose information is disclosed in violation of GLBA lack private right of action); Loring, *supra* note 54, at 448 (noting that GLBA does not provide consumer with cause of action against financial institution for wrongful disclosure).

128. No. 02 CIV.4687 (NRB), 2003 WL 21692820 (S.D.N.Y. July 21, 2003).

when Experian sold a customer's Social Security number and other identifiable information.[129]

Although the GLBA initially aimed to protect privacy, the watered-down version really does little to enhance protection of sensitive information. Financial institutions have sent out billions of notices without any change in privacy materializing.[130] Further, the defective nature of the GLBA, being "riddled with loopholes and exceptions," makes the consumer's ability to opt out ineffective.[131]

B. *HIPAA—Privacy for the Health Care Industry*

Ironically, even though Congress passed HIPAA before the GLBA, HIPAA carries much tougher privacy standards for the health industry.[132] HIPAA was enacted to facilitate health insurance transferability and the transfer of private information between entities.[133] Medical records contain some of the most sensitive personal information; however, more than seventeen organizations may handle a single medical record,[134] and approximately four hundred people may see a patient's medical record during one hospital stay.[135] According to some in the industry, "patient confidentiality is not eroding—it can't erode, because it's simply nonexistent."[136] A 1999 poll indicated that ninety percent of Americans feel that insurance companies' sharing records with other companies without con-

129. *See id.* at *3 (holding that Menton did not have cause of action because GLBA will be enforced by federal and state authorities and FTC only).

130. *See* Robin K. Warren, *GLB Privacy: More Than Just Consumer Notices*, SG066 ALI-ABA 61, 63 (2002) (stating that billions of notices have been sent by financial institutions); *see also* Hahn, *supra* note 100, at 130-31 (stating that over 2.5 billion privacy notices have been sent as of June 2001). For a discussion of the increase in identity theft caused by lack of privacy, see *supra* note 2 and accompanying text.

131. Pandozzi, *supra* note 22, at 234 (referring to flaws in GLBA as enacted).

132. *See* 45 C.F.R. § 160.103 (2003) (stating that regulations apply to "past, present, and future" health care transactions of individuals); *id.* § 164.502(a) (2003) (stating that information can only be disclosed to individual and otherwise authorization of individual is required); *see also* McLaughlin, *supra* note 62, at 1102 (noting that GLBA does not apply to former customers).

133. *See* Robert W. Woody, *Health Information Privacy: The Rules Get Tougher*, 37 TORTS & INS. L.J. 1051, 1051-52 (2002) (noting that idea of health information traveling between entities gave rise to privacy concerns).

134. *See Medical Records Privacy: Hearing on the Proposed Rule on the Privacy of Individually Identifiable Health Information Before the S. Comm. on Health, Educ., Labor & Pensions*, 107th Cong. (Apr. 26, 2000), *available at* 2000 WL 504626 (opening statement of Sen. Jeffords, Chairman, S. Comm. on Health, Educ., Labor, and Pensions) (stating that typical record can be seen by several individuals in more than seventeen different companies or organizations).

135. *See* Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 483 (2000) (noting that Congressional Research Service reported that approximately four hundred people see some portion of patient's medical record as result of one hospital stay).

136. Maggie Scarf, *Keeping Secrets*, N.Y. TIMES, June 16, 1996, § 6, at 38 (statement of Mark Hudson, former health insurance company employee).

sent is an invasion of privacy.[137] Accordingly, about one in six Americans takes affirmative steps to protect his or her privacy, such as paying out-of-pocket, rather than submitting personal information.[138] While Congress sought to protect the transfer of personal information, it did not directly create the privacy regulations—the Department of Health and Human Services (DHHS) created them.[139]

1. *Overview of Regulations*

a. HIPAA's Application

The HIPAA privacy provisions went into effect on April 14, 2003.[140] The HIPAA privacy provisions apply to all individually identifiable health information.[141] Interestingly, unlike the GLBA, the HIPAA privacy regulations apply to information from past transactions and customers.[142] Further, the HIPAA privacy provisions apply to a much broader range of entities than the GLBA; nevertheless, the GLBA does not supersede or limit any HIPAA regulations.[143] The HIPAA privacy provisions apply to health plans, health care clearinghouses and health care providers.[144]

137. *See* Scott, *supra* note 135, at 491 (reporting that 1999 poll indicated that ninety percent of Americans believe that sharing is invasion of privacy, and 1996 poll indicated that eighty-seven percent of Americans believe companies should get permission before sharing).

138. *See id.* at 493 (stating that one in six patients engages in privacy-protecting behaviors, such as switching doctors, paying out-of-pocket and other steps to ensure that his or her information is kept secret).

139. *See* Woody, *supra* note 133, at 1052 (noting that Congress instructed DHHS to create rules if Congress did not create them itself within thirty-six months). When Congress failed to act, DHHS set forth the current rules. *See id.* (discussing process for promulgating DHHS regulations).

140. *See* 66 Fed. Reg. 41316, 41341 (Aug. 7, 2001) (announcing DHHS's final rule regarding HIPAA, and setting compliance date to April 14, 2003) (to be codified 42 C.F.R. pts. 412 & 413).

141. *See* 45 C.F.R § 164.501 (2003) (defining individually identifiable information as including "(A) Name and address; (B) Date of birth; (C) Social Security number; (D) Payment history; (E) Account number"); *see also* 16 C.F.R. § 313.3(n) (2003) (stating vague standard of GLBA that protects nonpublic personal information, which is later defined as personally identifiable information).

142. *See* 45 C.F.R. § 160.103 (2003) (stating that regulations apply to "past, present, and future" health care transactions of individuals); *see also* 16 C.F.R. § 313.4(a) (2003) (stating that GLBA privacy applies to customers); McLaughlin, *supra* note 62, at 1102 (noting that GLBA does not apply to former customers).

143. *See* 16 C.F.R. § 313.1(b) (2003) ("Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of DHHS under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996 . . . .").

144. *See* 45 C.F.R. § 164.104 (2003) ("Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider . . . ."); *id.* § 160.103 ("Health plan means an individual or group plan that provides, or pays the cost of, medical care."). These entities can range from insurance companies to private health plans offered by employers, which broadens the applicability of the Act to the private business sector. *See id.*

The HIPAA regulations therefore also cover many of the entities covered by the GLBA, and those entities must comply with both statutes.[145]

Entities covered under the GLBA are also covered under HIPAA both directly and indirectly as third parties.[146] For example, if a bank performed a financial outsourcing service for a covered entity, it would be directly subject to the HIPAA privacy regulations.[147] Much like the GLBA, third parties that perform functions for a covered entity[148] are regulated by contractual agreements with the covered entity.[149] These agreements prevent the third party from disclosing personal information in violation

---

(including "[a]n employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers" under HIPAA regulations); William P. Matthews, *Caught Up in the Expanding Net: Regulation of the Business Associate Under the HIPAA Privacy Regulations*, 72 J. KAN. B.A. 32 (Apr. 2003) (noting that independent contractors, vendors and others not in health care industry, but who will or may obtain personal information are covered under HIPAA as "business associates").

145. *See supra* note 143 and accompanying text (stating that GLBA does not supercede or limit HIPAA). Therefore, HIPAA is the federal floor, and financial institutions would have to comply with any GLBA regulation that offers greater privacy. *See* Scott, *supra* note 135, at 515 (noting that HIPAA provides floor preemption, referencing fact that HIPAA does not displace stronger state privacy laws).

146. *See* Robert C. Lower & Michelle A. Williams, *Analysis of the Final HIPAA Privacy Regulations and Potential Implications for Financial Institutions*, 5 ELECTRONIC BANKING L. & COM. REP. 11 (Feb. 2001) (noting that financial institutions can become subject to HIPAA both directly and indirectly, depending on type of service provided). If financial institutions provide self-insured health plans for their employers, they are directly subject to HIPAA. *See id.* If, however, they perform certain data services for covered entities, they are indirectly subject to HIPAA as business associates. *See id.*

147. *See id.* at 11 (noting broad-reaching effects of HIPAA regulations); *see also id.* (stating that HIPAA will apply to financial institutions that "(1) provide health insurance services; (2) provide certain financial services to members of the health care industry; and (3) provide health insurance benefits for their employees").

148. *See* 45 C.F.R. § 160.103 (stating that business associate is person who provides "legal, actuarial, accounting, consulting, data aggregation, management" where this service involves personal information).

149. *See* 45 C.F.R. § 164.504(e)(1)(ii) (2003) (defining duty). The regulation states:

> A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

Id. (discussing when covered entity is noncompliant); *see also* Matthews, *supra* note 144, at 37 (recognizing that without addressing business associate, covered entities would be able to contract around HIPAA privacy provisions).

of the privacy provisions.[150] If a consumer paid for health treatment or insurance with a credit card, however, the financial institution would not be brought under the HIPAA regulations as a third party business associate.[151] Nevertheless, virtually all financial institutions provide health benefit plans for their employees and, therefore, become directly subject to the HIPAA privacy rules.[152]

Under HIPAA, if a third party breaches the contractual arrangement, the covered entity must take steps to correct the breach or terminate the contract.[153] Third parties themselves are not governed by the regulations, only by their contractual commitments.[154] The protections of the privacy rule pass through to the contracted business associates of the covered entity.[155] The covered entity is liable for unauthorized disclosures by a third party if the covered entity had actual knowledge of material violations.[156] This liability only requires that the entity terminate the contract.[157] At the

150. *See* Matthews, *supra* note 144, at 40 (explaining how requirement expands business associate's obligations beyond actual agreement and incorporates by reference all privacy provisions).

151. *See* Lower & Williams, *supra* note 146, at 5 (noting HIPAA privacy regulations do not classify financial institution as business associate when financial institution processes credit card payment); Diana J.P. McKenzie & Benjamin D. Kern, *Privacy and Outsourcing: The Regulatory Framework*, 724 PRAC. L. INST. 341, 355 (2002) (stating that financial institutions are not business associates because they act as conduit for protected information by transmitting information, but financial institutions are not intended to access information).

152. *See* Anne Wallace, *The Impact of HIPAA on Financial Institutions*, 56 CONSUMER FIN. L.Q. REP. 231, 232 (2002) (stating that virtually all financial institutions provide group medical, dental, vision and health spending accounts, which are health plans under HIPAA privacy provisions).

153. *See* 45 C.F.R. § 164.504 (stating that covered entity can be responsible if entity had actual knowledge of business associate misconduct).

154. *See* Woody, *supra* note 133, at 1069 (noting that third party obligations arise only on contractual responsibilities and suggesting that this will lead to litigation concerning who is responsible for unauthorized third party disclosures).

155. *See* Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 419 (2003) (claiming that privacy rule clearly passes through to business associates and that business associates are under same duties as covered entities when dealing with personal information); Matthews, *supra* note 144, at 40 (stating that HIPAA contractual provisions incorporate by reference privacy standards to third party business associate).

156. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,252 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160 & 164) (stating that "the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation"); *see also* 45 C.F.R. § 164.504(e)(1)(ii) (2003) (holding covered entity responsible when it knew of material breach, unless it took reasonable steps to cure breach or violation); Matthews, *supra* note 144, at 41 (stating that covered entity has actual knowledge when it has substantial evidence of violations).

157. *See* 45 C.F.R. § 164.504(e)(1)(ii) (stating that if breach cannot be reconciled, covered entity must terminate relationship, and if infeasible to terminate, report third party to DHHS); Matthews, *supra* note 144, at 40-41 (recognizing that

conclusion of the contractual relationship, the third party must destroy any personal information received from its association with the covered entity.[158]

b. Authorization Requirements Before Disclosure—The Opt-In Provision

Like the GLBA, HIPAA requires covered entities to send a privacy notice that states the entities' policies for sharing personal information without consent.[159] A covered entity may disclose personal information only with the consent or authorization of the patient.[160] This opt-in provision prohibits any disclosure without prior explicit authorization unless an exception applies.[161] A patient must clearly write and sign an authorization.[162] No authorization is required for disclosures made for certain marketing purposes.[163] An opt-out option, however, is still provided, and only the "minimum necessary" information to accomplish the purpose of the transaction may be disclosed.[164]

---

termination of business-associate agreement is extent of remedy available after covered entity has taken reasonable steps to attempt to end breach of privacy contract).

158. *See* 45 C.F.R. § 164.504(e)(2)(ii)(I) (stating that at conclusion of relationship, business associate must destroy personal information, and if it is not feasible to destroy, business associate must continue to protect information); Wallace, *supra* note 152, at 234 (noting that HIPAA requires that records be destroyed or returned to covered entity at completion of contractual relationship; if personal information cannot be destroyed or returned then it must continue to be protected under provisions of contract).

159. *See* 45 C.F.R. § 164.520(b) (2003) (stating notice requirements and that HIPAA notice must include following statement prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY").

160. *See id.* § 164.502(a) (2003) (stating that information can only be disclosed to individual and that, for other disclosures, authorization of individual is required); *id.* § 164.508(c)(1) (2003) (stating that authorization must be specific and identify information that is to be disclosed, to whom it will be disclosed and for what purpose it will be disclosed).

161. *See id.* § 164.512 (2003) (noting list of HIPAA exceptions, including marketing, public safety and treatment purposes); *id.* § 164.514(e) (2003) (stating that only opt-out requirement is required for marketing purposes).

162. *See id.* § 164.508(c)(3) (providing that "[t]he authorization must be written in plain language").

163. *See id.* § 164.508(a)(3) (stating that no authorization is needed to disclose personal information for marketing services if marketing is face-to-face or if marketing is for promotional gift of nominal value that is provided by covered entity); *see also* Woody, *supra* note 133, at 1065 (stating that covered entity must determine that product is beneficial to person being targeted, and covered entity must inform individual why individual was targeted).

164. *See* 45 C.F.R. § 164.502(b)(1) (stating that "a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request"); Matthews, *supra* note 144, at 40 (noting that minimum necessary standard also applies to disclosures that are authorized).

c. Criticisms of HIPAA Privacy Protections

Privacy advocates are concerned that the exceptions to the privacy regulations will undermine HIPAA's overall scheme, and some advocates feel that HIPAA offers little privacy protection.[165] Under HIPAA, an entity can disclose personal information for its own health care operations, including patient care and billing services.[166] The "good faith" notice requirement permits entities to design business-friendly notices, which may fail to inform the patient.[167] Critics of HIPAA also argue that many patients will likely sign authorization forms without reading them.[168] Another concern is that DHHS did not define the "minimum necessary" standard for information that is disclosed.[169] Confusion also arises about the extent of the "reasonable efforts" required to reduce personal information to the "minimum necessary" standard.[170] Therefore, HIPAA allows the covered entity to judge how much personal information it should disclose.

On its face, HIPAA sets relatively strong privacy provisions, yet it does not have an adequate enforcement mechanism.[171] The HIPAA regula-

165. *See* 142 CONG. REC. H9785, 9792 (daily ed. Aug. 1, 1996) (statement of Mr. McDermott) (stating that there is "not one single shred of protection of your privacy" under HIPAA privacy provisions); Mary K. Martin, *Some Things Old, Some Things New: The HIPAA Health Information Privacy Regulations*, 59 BENCH & B. MINN. 32 (2002) (noting that existing laws in some states provide greater protections than HIPAA).

166. *See* 45 C.F.R. § 164.506 (2003) (stating that "a covered entity may use or disclose protected health information for treatment, payment, or health care operations").

167. *See* Jennifer Guthrie, *Time Is Running Out—The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices*, 12 ANNALS HEALTH L. 143, 172-73 (2003) (arguing that relaxed procedures could potentially fail to provide patients with privacy information, and noting that simple signature in log book could be sufficient to meet "good faith effort" acknowledgment requirement of privacy rule).

168. *See* Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497, 1504 (2002) (stating that it is well known that patients sign forms without understanding them). Many hospitalizations and medical procedures carry with them an inherent level of stress, which may impair the patient's comprehension of the notice. *See* Kutzko, *supra* note 155, at 410 (noting that one-time notice, provided during high stress time of admission, may not be sufficient for patient to form basis of knowing waiver).

169. *See* 45 C.F.R. § 164.502(b)(1) ("When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."); Jacobson, *supra* note 168, at 1505 (noting ambiguity and difficulty in determining what "reasonable efforts" and "minimum necessary" mean in practice).

170. *See* Guthrie, *supra* note 167, at 166 (arguing that DHHS created "more confusion than assistance" by requiring that covered entities use input of prudent professionals in order to achieve compliance with privacy provisions, and suggesting that DHHS clarify level of reasonableness required so that covered entities may establish policies and procedures).

171. *See* 45 C.F.R. § 164.501 (2003) (defining stringent guidelines of HIPAA compliance); *see also* Winn, *supra* note 93, at 618 (stating that HIPAA does not

tions carry strong penalties for unauthorized disclosures, including fines of up to $250,000 and sentences of up to ten years in prison.[172] Administrative agencies enforce HIPAA, and individuals have no private cause of action.[173] Compounding this problem is the fact that third parties are not subject to legal sanctions, even though these third parties are businesses responsible for many of the abuses of personal information.[174]

HIPAA privacy provisions also come under attack for their marketing exceptions.[175] Authorization is not required for goods or services of a nominal value.[176] HIPAA critics have suggested that a marketer could get personal information by offering a fifty-cent coupon.[177] Another marketing exception is that no authorization is required for health-related products or services of the covered entity.[178]

The largest complaint from the health care industry focuses on the costs of implementing privacy protections.[179] The strict HIPAA privacy regulations are estimated to cost over $3 billion for compliance in the first year.[180] Nevertheless, bipartisan support exists for protecting privacy de-

provide federal cause of action to remedy violations, but, rather, patients must rely on administrative process). Perhaps even more alerting, business associates are not subject to HIPAA sanctions, yet evidence indicates that they are often responsible for abuses of personal information. *See id.* (listing common criticisms of HIPAA).

172. *See* 42 U.S.C. § 1320d-6 (2003) (stating that "if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, [the offender shall] be fined not more than $250,000, imprisoned not more than 10 years, or both").

173. *See* Winn, *supra* note 93, at 618 (noting that HIPAA rules do not create federal cause of action for those injured through violation of rules); *see also* Loring, *supra* note 54, at 448 (noting that GLBA does not provide consumer with cause of action against financial institution for wrongful disclosure).

174. *See* Winn, *supra* note 93, at 618 (noting that business associates are not subject to legal sanctions of HIPAA rules, and finding this fact troubling because these business associates appear responsible for many of abuses of personal information that led Congress to consider Act in first place).

175. *See* 45 C.F.R. § 164.508(a)(3) (2003) (stating marketing exceptions allow exception from HIPAA requirements for face-to-face marketing technique and gifts of nominal value).

176. *See id.* § 164.508(a)(3)(i) (stating that authorization is not required for marketing when communication is in form of promotional gift of nominal value that is provided by covered entity or when face-to-face marketing occurs).

177. *See* James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. REV. MICH. ST. U. DETROIT C.L. 855, 870 (suggesting that marketers could get personal information by offering pencils, coupons and various other low cost items).

178. *See* 45 C.F.R. § 164.514(f)(1) (2003) (stating that covered entity may use or disclose protected information for purposes of fundraising); *id.* § 164.501 (2003) (stating that marketing includes communications relating to health products and services provided by covered entity).

179. *See generally* Jacobson, *supra* note 168, at 1503 (noting that from industry perspective, HIPAA will be very costly and that government cost estimates are much lower than industry cost estimates).

180. *See* Scott, *supra* note 135, at 513 (stating that federal officials estimate HIPAA compliance to cost $3.2 billion, while those in industry expect compliance

spite costs to the health care industry.[181] Moreover, analysts suggest that the high-cost estimates associated with HIPAA compliance are linked to the exponential growth of electronic record keeping with little regard for previous duties of confidentiality.[182] The relatively stringent HIPAA privacy standards generated constitutional challenges to DHHS's authority to promulgate such rules.[183] Furthermore, parties challenged the HIPAA regulations for vagueness.[184] Despite these challenges, HIPAA went into effect unscathed.[185] Although HIPAA survived, so do the challenges it presents for consumers wishing to safeguard their personal information.[186]

V. Suggested Reforms

GLBA and HIPAA are statutes that aim to protect consumers' personal information. Extreme privacy regulations, however, may actually injure consumers by denying them valuable services.[187] Both GLBA and HIPAA strive to protect personal information while allowing consumers to enjoy the benefits available in the information age. Both laws, however, contain loopholes that allow entities to disseminate personal information to third parties. In the arena of identity theft, any dissemination of per-

to cost many times that amount); *see also* Mary Beth Johnston, *HIPAA Becomes Reality: Compliance with New Privacy, Security, and Electronic Transmission Standards*, 103 W. Va. L. Rev. 541, 552 n.64 (2001) (noting that 1999 Blue Cross/Blue Shield survey estimated HIPAA privacy compliance costs at $43 billion).

181. *See* Winn, *supra* note 93, at 640-41 (noting that HIPAA regulations have gone through two political administrations, and indicating bipartisan support for increased protection of privacy even if it involves significant costs to health care industry).

182. *See id.* at 680 (suggesting that high costs associated with HIPAA privacy appear to be due to "exponential growth in use of electronic health information" without corresponding growth in "existing duties of confidentiality," implying that compliance with HIPAA rules is simply wake-up call to health industry that explosion of electronic information also carries potential dangers).

183. *See* S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 352-55 (4th Cir. 2003) (holding that it was not unconstitutional for DHHS to set privacy standards).

184. *See id.* (finding that regulations are not unconstitutionally vague).

185. *See id.* at 352-55 (holding that it was not unconstitutional for DHHS to set privacy standards, that protections can extend to nonelectronic record information and that statute and regulations are not unconstitutionally vague); Ass'n of Am. Physicians & Surgeons v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115, 1124 n.5, 1126 n.7 (S.D. Tex. 2002) (finding that HIPAA did not preempt state laws that are not contrary to privacy rule if state rule is more stringent and that HIPAA falls within congressional Commerce Clause authority to regulate interstate commerce).

186. *See* Molenaar, *supra* note 177, at 857-58 (noting that HIPAA privacy regulations are largely ineffective because of loopholes).

187. *See* Scott, *supra* note 135, at 494-95 (discussing Maine privacy law that was so stringent that it prevented hospital personnel from giving patient information to family and friends over phone, blocked delivery of flowers to patients and prevented doctors from comparing patient notes without patient consent). The law was repealed within two weeks of its enactment and replaced. *See id.* (explaining results of "too much" privacy).

sonal information increases the risk of theft.[188] Since the passage of HIPAA and the GLBA, identity theft has continued to soar to record levels.[189] To effectively curb the increase in identity theft, Congress should use HIPAA as an initial framework, and with several modifications, HIPAA and the GLBA can work together to prevent the theft or dissemination of personal information from large financial and health care institutions.[190]

A. *Adopt the HIPAA Opt-In Standard*

Because of the difficulty of opting out, Congress should modify the GLBA to include an opt-in system. Although many Americans are concerned about their privacy, less than five percent choose to opt out of information sharing.[191] On the other hand, 52.8 percent of adults choose not to have their information shared when presented with an opt-in option.[192] Statistics suggest that the opt-out provisions are not enough and that the average consumer cannot or does not read and understand them.[193] Polls indicate that a vast majority of Americans prefer an opt-in system.[194] A recent vote in North Dakota corroborated the polls' results when seventy-two percent of the residents voted for an opt-in system.[195] The argument that switching to an opt-in system would be too expensive is

188. *See* Hoofnagle, *supra* note 74, at 206 (giving examples that show that every time information is shared, opportunity for identity theft increases).

189. For a further discussion of the rise in identity theft, see *supra* note 2 and accompanying text.

190. *See* Hickerson, *supra* note 79, at 797 (noting that HIPAA provides initial framework for expanding privacy protections beyond medical records and into financial industry); *see also* Lower & Williams, *supra* note 146, at 11 (noting that many financial institutions are already brought under HIPAA both directly and indirectly).

191. *See* Hahn, *supra* note 100, at 150 (stating that according to one study, only three percent of adults in 2002 chose to opt out of centralized information sharing).

192. *See id.* at 149 (noting that 48.2 percent of adults chose to have their information shared under opt-in system, leaving personal information of 52.8 percent of adults unshareable).

193. *See id.* (noting that under opt-out system 96.3 percent of people did not respond, thus allowing vast majority of information to be shared, and stating that under opt-in system, 48.2 percent chose explicitly to have their information shared). This discrepancy shows that individuals want their information protected, but are unable to do so under an opt-out system. *See id.* (explaining consumer trend).

194. *See* Hoofnagle, *supra* note 74, at 205 (reporting that ninety-three percent of Americans believe that permission should be received before sharing).

195. *See id.* (citing March 2000 *BusinessWeek*-Harris poll that indicated eighty-eight percent of Internet users wanted to opt in before Web sites shared their information and that 1991 *Time*-CNN poll indicated that ninety-three percent of respondents believed companies should get permission before sharing). Another poll reported that on June 11, 2002, seventy-two percent of North Dakota residents voted for an opt-in system despite the banking industry spending over $100,000 to oppose the vote. *See id.*

flawed because the expense can be offset by the tens of billions of dollars a year that companies would otherwise lose to identity theft.[196]

Opponents of the opt-in system argue that there is no difference between opting in and opting out because a consumer still has a choice under both systems.[197] However, if the consumer does not understand the notice, setting the nonresponse default to protect personal information is the safest and most cautious means of protecting privacy.[198] The financial services industry and the health care industry argue that opt-in systems are more burdensome because they must contact each customer.[199] This argument fails because under both the GLBA and HIPAA, entities must contact each customer with an opt-out provision.[200] Information advocates contend that the opt-in system is more intrusive because it requires companies to contact customers continually to gain their permission to share information.[201] If opting in is more intrusive, Congress could ameliorate the intrusiveness by only allowing institutions to send opt-in notices with their required annual privacy notices under the GLBA.[202] Nevertheless, the risk of losing personal information outweighs the expenses of complying with the law.[203]

1. *The Alleged Adverse Impacts of an Opt-In Scheme—The MBNA Case Study*

In 2002, Professor Cate of Indiana University School of Law launched a case study into the effect an opt-in scheme would have on a large financial institution, namely, MBNA.[204] MBNA is an extreme case because it

196. *See* FTC REPORT, *supra* note 2, at 7 (finding that identity theft costs businesses, including financial institutions, $47.6 billion annually).

197. *See* Zielezienski, *supra* note 69, at 352 (noting that opt-in system provides consumers with choice, but arguing that this is less of choice because it assumes that consumers prefer privacy over benefits of goods and services available).

198. *See supra* note 71 and accompanying text (noting benefit opt-in system brings by not requiring consumers to read through long documents).

199. *See* Zielezienski, *supra* note 69, at 352 (discussing cost burden of opt-in system).

200. *See id.* (arguing that opt-in system is inherently more costly to implement because it requires contacting each customer directly as opposed to contacting all customers at once). *But see* Givens, *supra* note 73 (arguing that opt-in costs are not substantial compared to opt-out requirements).

201. *See* Zielezienski, *supra* note 69, at 352 (arguing that opt-in scheme is more intrusive because it requires more contacts before company can get consent to share information). *But see* Givens, *supra* note 73 (stating that cost for opt-in system is not as high as analysts claim).

202. *See* 16 C.F.R. § 313.4(a) (2003) (requiring financial institutions to provide clear and conspicuous notice to customers, and these notices must be sent initially as well as annually).

203. *See* Fred H. Cate & Michael E. Staten, The Privacy Leadership Initiative, *The Adverse Impact of Opt-In Privacy Rules on Consumers: A Case Study of Retail Credit* (Apr. 2002), *at* http://www.bbbonline.org/UnderstandingPrivacy/library/whitepapers/RetailCreditStudy.pdf (discussing case study to demonstrate costs and benefits of complying with GLBA).

204. *See id.* at 3 (noting that MBNA achieved its success by collecting personal information and then targeting potential customers with credit packages).

bases all its operations on the collection and analysis of personal information.[205] By targeting individuals with common interests, MBNA used personal information to build its customer base to fifty-one million individuals.[206] MBNA's use of personal information allowed it to target geographic markets with astounding speed.[207] Professor Cate argued that an opt-in scheme would severely affect both MBNA and consumers.[208]

Professor Cate argued that a third party opt-in scheme would harm MBNA because it would reduce the amount of personal information the company received from external sources.[209] Cate also suggested that an opt-in scheme, related to affiliate sharing, would adversely affect MBNA because MBNA is organized into eight divisions for tax and logistical purposes.[210] The perceived injuries to MBNA were attributed to the low response rate of individuals under an opt-in scheme.[211] U.S. West undertook a study and determined that it took an average of 4.8 calls and twenty dollars before an adult could be reached to give consent under an opt-in system.[212] Cate argued that such an opt-in system would effectively end MBNA's marketing approach by significantly restricting the personal

---

205. For a further discussion of the MBNA business model, see Cate & Staten, *supra* note 203 (discussing case study of MBNA).

206. *See* Cate & Staten, *supra* note 203, at 8 (noting that MBNA provides credit card or loan services to fifty-one million consumers and has $89 billion in outstanding loans).

207. *See id.* at 9 (stating that by acquiring information about cardholder prospects, MBNA was able to target potential customers and enter market with astounding speed). Also, the key to the company's success was its screening of customer interests to identify individuals who would be likely customers. *See id.* at 13 (explaining why availability of personal information is necessary to maintain competitive edge).

208. *See id.* at 3 (noting negative effect on businesses and consumers under opt-in system).

209. *See id.* at 27 (noting that company depends on external sources to develop customer leads).

210. *See id.* at 16-17 (noting that MBNA is divided into eight separate divisions for tax and insurance purposes and that customers are often unaware of legal distinctions that make these divisions affiliates).

211. *See id.* at 18 (noting that fifty-two percent of unsolicited mail goes unread, leading to opt-in response rates of five to eleven percent); *see also* Hahn, *supra* note 100, at 149 (stating that under opt-in tests, 48.2 percent of adults affirmatively responded and shared their information).

212. *See* Cate & Staten, *supra* note 203, at 19 (noting that in U.S. West study, it took average of 4.8 calls to reach household and one-third of households were never reached). Of those households that were reached, twenty-eight percent chose to share their information, in addition to the five to eleven percent that shared via direct mail. *See id.* (relating findings of U.S. West study). When customers were asked to opt in during a call initiated by the customer, the opt-in rate was seventy-two percent. *See id.* (noting significant differences resulting from opt-in scheme).

information available.[213] MBNA argued that consumers would be unable to receive services they desire.[214]

MBNA collected personal information to create an annual list of 800 million possible customers and then cut the list to 400 million individuals who were likely to become customers.[215] The average response rate for a direct mail credit card offer was 0.6 percent.[216] Professor Cate reported that if all the information used to dilute MBNA's initial list were suppressed, MBNA would cut the list to 550 million instead of 400 million.[217] MBNA argued that the inclusion of the extra 150 million potential customers would result in a loss of eight percent of pre-tax income on each new account over a five-year period, as MBNA reverts to a blind mass marketing scheme.[218]

Although Professor Cate's argument concerning the financial well-being of MBNA illustrates the importance of information in today's society, it overstates the costs that an opt-in system would create.[219] MBNA bases its business model entirely on the collection of personal information, which is not representative of businesses as a whole. Although many businesses collect personal information, few utilize it as much as MBNA does, so MBNA can be classified as a worst-case scenario.[220] Further, when calculating the potential loss to MBNA, Professor Cate assumed that an opt-in system would prevent MBNA from acquiring any personal information.[221] The numbers demonstrate that this is not the case because when an opt-in scheme is initiated by telephone, the positive response rate is between

213. *See id.* at 20 (stating that increased cost combined with low response rate would sharply limit organizations' ability to share their personal information lists with MBNA).

214. *See id.* at 19 (stating that those who failed to opt in missed opportunities to receive services).

215. *See id.* at 22 (noting MBNA business model of using personal information to target four hundred million individuals who are likely to become customers).

216. *See id.* at 37 n.42 (stating that BaiGlobal, Inc. reported that credit card companies issued 3.53 billion credit card offers in 2000, receiving response rate of 0.6 percent).

217. *See id.* at 24 (noting that MBNA study revealed that without gathered personal information, potential customer list would only be cut to 550 million).

218. *See id.* at 25-26 (stating that inclusion of those who would have been eliminated causes twenty-two percent increase in cost per account opened, which Professor Cate translates into eight percent over five years).

219. *See* Givens, *supra* note 73, ¶ 53-55 (arguing that cost of opt-in scheme is similar to cost of opt-out scheme).

220. *See* Cate & Staten, *supra* note 203, at 9 (stating that by acquiring information about cardholder prospects, MBNA was able to target potential customers and enter market with astounding speed).

221. *See id.* at 19 (assuming that opt-in scheme blocks all information).

twenty-eight and seventy-two percent.[222] Therefore, it is likely that MBNA would still acquire a substantial amount of the information it needed.[223]

The costs associated with getting opt-in authorization would not be levied against MBNA because MBNA is a third party.[224] Nevertheless, there are cost-effective ways of getting opt-in consent.[225] Furthermore, the costs associated with achieving consent are a one-time expense, the benefits of which businesses can enjoy for years ahead.[226] This initial cost is a small price to pay in an industry that has lost substantial revenue from identity theft.[227] Furthermore, with the response rate from direct mail being miniscule, the argument that consumers will not receive the services they desire is trivial.[228] Therefore, even in a worst-case scenario, an opt-in system allows business to continue and substantially increases consumer protection.[229]

B. *Eliminate Unauthorized Sharing with Affiliates, Third Parties and Marketers*

Both the GLBA and HIPAA have similar flaws because they allow entities to share personal information with affiliates without consent.[230] The

222. *See id.* at 19 n.32 (noting that residential customers opted in at rate of twenty-eight percent when called and at rate of seventy-two percent when customer initiated call).

223. *See id.* (noting high response rate possible under opt-in system).

224. *See* Pandozzi, *supra* note 22, at 200 (noting third parties are not subject to GLBA).

225. *See* Cate & Staten, *supra* note 203, at 19 n.32 (noting that when customer initiates transaction, opt-in rates are over seventy percent).

226. *See* Zielezienski, *supra* note 69, at 315 (noting that once customer opts in, information can be shared).

227. *See* Cate & Staten, *supra* note 203, at 24-25 (noting that if average response rate were 0.6 percent, MBNA would only be able to cut its potential customer list to 550 million instead of 400); *id.* at 3 (noting that MBNA handles fifteen percent of Visa/MasterCard customers); Hoar, *supra* note 2, at 1425 (noting that Secret Service estimated that identity theft cost financial institutions $745 million in 1997 and MasterCard reported identity fraud cost its member banks $407 million); U.S. Postal Serv., *Discount Mailing Services, at* http://pe.usps.gov/text/dmm200/discount.htm (last visited Nov. 25, 2003) (stating that bulk rate for first class letter can be as low as 0.275 cents when pre-sorted by carrier route). For example, assuming that MBNA has no personal information and sends out the extra 150 million card offers, it would cost $40.5 million in postage minus the revenue generated by the nine hundred thousand new customers MBNA would pick up based on average response rate. *See* Cate & Staten, *supra* note 203, at 25 (describing MBNA response rates). Compare that figure with the fact that MBNA loses at least $60.5 million a year through identity theft based on its fifteen percent control of MasterCard (who lost $407 million). *See id.* at 3 (stating that MBNA controls fifteen percent of Visa/MasterCard accounts).

228. *See* Cate & Staten, *supra* note 203, at 24-25 (noting response rate is 0.6 percent).

229. *See supra* note 71 and accompanying text (noting major benefit of opt-in system).

230. *See* Horn, *supra* note 55, at 100-01 (noting that GLBA privacy provisions do not apply to affiliates or to third parties who perform services for covered en-

laws should be regulated by an opt-in system before the information is disseminated.[231] A simple check-box card, which allows consumers to check the affiliates with whom they would like to share their information, could implement this system.[232] Entities could send this card as part of the annual privacy notice package.[233]

The contractual relationships employed by both the GLBA and HIPAA do not provide any security.[234] If a third party decides to sell the information, there is little the consumer or covered entity can do besides canceling the contract.[235] Therefore, when entities make these contractual arrangements, there should be a mandatory clause in the contract stating that the third party is independently subject to the GLBA or HIPAA.[236]

HIPAA's marketing exception undercuts the law's efficacy.[237] There seems to be no logical reason to allow marketers to have access to personal information.[238] The information given to marketers should be limited to names, addresses and a preferred product.[239] Nevertheless, marketers

---

tity); Matthews, *supra* note 144, at 40-41 (recognizing that termination of business associate agreement is extent of remedy available, if associate breaches privacy provisions).

231. *See supra* note 71 and accompanying text (noting benefit opt-in system brings by not requiring consumers to read through long documents).

232. *See* Cuaresma, *supra* note 74, at 603 (noting that easier procedures include availability of toll-free numbers, web sites and check boxes on postcards to facilitate process).

233. *See* 16 C.F.R. § 313.4(a) (2003) (requiring financial institutions to provide clear and conspicuous notice to customers, and these notices must be sent initially as well as annually).

234. *See generally* Pandozzi, *supra* note 22, at 200 (noting that "a financial institution may entirely circumvent [GLBA] by entering into [such] contracts with third-party service providers").

235. *See generally* 45 C.F.R. § 164.504(e)(1)(ii) (2003) (stating that if breach cannot be reconciled, covered entity must terminate relationship).

236. *See* Matthews, *supra* note 144, at 40 (stating that HIPAA contractual provisions incorporate by reference privacy standards to third party business associate). *But see* 45 C.F.R. § 164.104 (2003) ("Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider . . . ."). Therefore, there is no enforcement mechanism for third parties. *See id.*

237. *See* Scott, *supra* note 135, at 511 (discussing concerns raised by Health Privacy Project concerning loopholes in marketing); *see also* Pandozzi, *supra* note 22, at 200 (arguing that third party services and marketing exceptions allow information to flow free of privacy regulations, in reference to GLBA marketing exceptions).

238. *See* Pandozzi, *supra* note 22, at 200 (arguing that, unknown to consumer, third party services and marketing exceptions could theoretically allow third parties to reuse information and retransfer personal information to more nonaffiliated third parties, thus bypassing all of GLBA privacy protections).

239. *See id.* (discussing harm when third parties possess personal information).

should only be given personal identifiable information that is public and should be brought under HIPAA by a contract provision.[240]

C. *Eliminate Social Security Numbers from All Sharing and Actively Prosecute Companies That Make Unauthorized Disclosures*

Social Security numbers are the biggest resource for identity thieves.[241] Consumers have become sensitive to distribution of their Social Security numbers.[242] Courts have held that a credit-reporting agency cannot force a consumer to provide a Social Security number.[243] A marketer usually has little need for a Social Security number.[244] If consumers authorize companies to share information, the Social Security number on a consumer's file should be protected to prevent identity theft.[245] Privacy advocates have suggested that institutions use an alphanumeric number for each of their customers instead of using a Social Security number because any number can be used for file identification.[246] HIPAA hints at this concept and requires that companies only disclose the minimum necessary information.[247] This concept should be better defined and expanded to those institutions covered by the GLBA.[248]

240. *See* Matthews, *supra* note 144, at 40 (stating that HIPAA contractual provisions incorporate by reference privacy standards to third party business associate, therefore, providing partial incentive for marketers to keep information they have private or risk contract termination).

241. *See supra* note 15 and accompanying text (describing use of Social Security numbers in identity theft).

242. *See* Sabol, *supra* note 13, at 166 (noting importance of Social Security numbers and their large role in crime of identity theft); *see also* Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 805 n.14 (2003) (listing several bills that have been proposed in Congress to protect use of Social Security numbers, such as protecting use of Social Security numbers in commercial transactions without consent).

243. *See* Menton v. Experian Corp., No. 02 Civ. 4687(NRB), 2003 WL 21692820, at *4 (S.D.N.Y. July 21, 2003) (finding that Menton refused to give his Social Security number to Experian because Experian made no promise of confidentiality; thereafter Experian refused to furnish Menton with copy of his credit report); *id.* at *5 (holding that nothing prevented Experian from furnishing Menton with his credit report without submitting his Social Security number).

244. *See supra* note 15 and accompanying text (discussing misuse of Social Security numbers as a de facto national identifier); *see also* Sabol, *supra* note 13, at 166 (discussing attractive nature of Social Security numbers to thieves).

245. *See* Sabol, *supra* note 13, at 166 (noting that Social Security numbers are attractive to thieves).

246. *See generally* Wendy Wuchek, *Conspiracy Theory: Big Brother Enters the World of Health Care Reform*, 3 DEPAUL J. HEALTH CARE L. 293, 295-96 (2000) (noting that HIPAA calls for DHHS to develop national record identifier, and there have been several proposals for this number, including keeping Social Security number, alphanumeric numbers, picture and biometric identifiers).

247. *See supra* note 144 and accompanying text (describing privacy requirements under HIPAA).

248. *See* 16 C.F.R. § 313.3(k)(1) (2003) (defining financial institution as business that is "significantly engaged" in financial activity).

With identity theft at its highest level in history, it is readily apparent that thieves are easily accessing personal information.[249] The FTC and DHHS are each in charge of enforcing the GLBA and HIPAA.[250] Despite the rise in identity theft and the vast penalties available, virtually no individual or company has been charged with violating either of the statutes.[251] Understandably, the FTC and DHHS may be wary of filing charges because of the floodgate of litigation charges that could follow.[252] If the agencies do not feel that they can handle the flood, they should allow a private cause of action only for egregious or intentional violations.[253] The possibility of private actions should have a strong deterrent effect on institutions that gather personal information.[254] Effective enforcement is necessary to curb the proliferation of identity theft, which otherwise will cost consumers and the financial industry billions annually.[255]

VI. CONCLUSION

Identity theft has grown to epidemic levels, and current law has proven ineffective in correcting the problem.[256] Therefore, Congress must correct the privacy provisions of the GLBA and HIPAA to protect personal information at central sources.[257] Congress must amend its current laws to prohibit third party sharing, implement an opt-in system and restrict use of Social Security numbers.[258] Identity theft will continue to

249. *See supra* note 2 and accompanying text (discussing rapid rise in identity theft).

250. *See* 45 C.F.R. § 160.506 (2003) (stating that Secretary of DHHS shall impose penalties for violations of HIPAA); *see also* Centralized Complaint and Consumer Education Service for Victims of Identity Theft, Pub. L. No. 105-318, § 5, 112 Stat. 3007 (2003) (charging FTC with enforcing GLBA).

251. *See supra* note 2 and accompanying text (noting that there have been millions of victims, yet few arrests).

252. *See supra* note 2 and accompanying text (discussing fact that millions of people have been victims of identity theft).

253. *See supra* note 83 and accompanying text (noting harsh penalties already prescribed under GLBA for intentional violations).

254. *See* Cuaresma, *supra* note 74, at 514 (noting that there is little incentive to comply because lack of private cause of action does not create threat of large monetary damages).

255. *See supra* note 4 and accompanying text (discussing enormous costs of identity theft).

256. *See supra* note 2 and accompanying text (discussing rapid rise in identity theft).

257. *See supra* note 53 and accompanying text (discussing fact that identity thieves gather personal information from large, centralized sources).

258. *See* Sabol, *supra* note 13, at 166 (noting that Social Security numbers are attractive to thieves).

occur at alarming rates until the law develops an effective approach to protecting personal information.[259]

R. Bradley McMahon

259. *See supra* note 2 and accompanying text (discussing soaring identity theft levels).